ELECTRONIC SECURITY COMPONENT

Field of the Invention

The present invention relates to electronic devices, and, more particularly, to an electronic security component in which sensitive information is processed.

Background of the Invention

Electronic security components processing sensitive information are used especially in smart cards. Applications of these cards include accessing banks for banking applications, and for remote payments for television, gasoline distribution and highway tolls, for example. These electronic security components have to process confidential data that must be shielded against any attempt at espionage for fraudulent purposes. The confidential data travels through the data bus of the component between a central processing unit (processor) and peripherals, such as memories.

Different methods can be implemented to discover these confidential data elements. In particular, one physical characteristic that can be observed external the electronic component is its current signature which depends on the passage of data in transit on the data bus. The data bus has a high

capacity because it circulates throughout the component.

For this reason, the output interface includes three-state selection switches sized to let through high current for charging or discharging the line capacitor. Since the data bus is an 8-bit data bus, it includes eight large selector switches that are activated to apply a data element to this bus. Consequently, there is high current consumption during the selection switching of the switches.

Summary of the Invention

In view of the foregoing background, it is an object of the present invention to prevent the identification of data elements traveling through the bus or at least make this identification difficult.

It is another object of the present invention to use data encryption to improve the protection of confidential data.

Yet another object of the present invention is to implement data encryption at low cost whether in terms of silicon surface area, connection lines between the peripherals and the central processing unit, or data-processing time.

Another object of the present invention is to implement a data encryption system that can be adapted to all classes of components in a relatively straight forward manner without extra cost of customized design.

In view of these and other objects, advantages and features, one approach is to provide a component whose central processing unit and peripherals, which have to process sensitive data received or transmitted on the data bus, each comprise an encryption/decryption cell. Each encryption/decryption cell applies the same secret key produced locally by each cell at each clock cycle to a

data element received or to be transmitted in the clock cycle.

Using the convention according to a clock cycle starting at the high level, the writing of a data element of the bus is done at the low level and the reading of a data element on the bus is done on the leading edge. Thus, in a given clock cycle, a data element may be encrypted with a secret key produced by the cell of a sender and transmitted on the bus during the write period on the bus. This encrypted data element may be read by an addressee and decrypted in the cell of this addressee with the secret key locally produced by this cell.

The two locally produced secret keys have the particular feature of being identical. Thus, according to the invention, the secret key is produced locally in each cell from a synchronous random signal applied to all. This is done in one clock cycle for the encryption of a data element given by a sender, and for the decryption of this data element encrypted by an addressee.

The present invention therefore relates to an electronic component comprising a two-way bus through which data elements travel in transit between peripherals and a central processing unit at the rate of a clock signal. The central processing unit and at least one of the peripherals each comprises a data encryption/decryption cell using the same secret key. A current value of the secret key is produced locally in each cell at each clock cycle from a random signal synchronous with the clock signal, and is applied to each of the cells by a one-way transmission line.

Brief Description of the Drawings

Other features and advantages of the invention shall be described in detail in the following

description by way of a non-restricted indication and with reference to the appended figures, of which:

Figure 1 shows an exemplary architecture of an electronic component to which the present invention can be applied;

Figure 2 shows a simplified architecture of an electronic component according to the present invention;

Figure 3 is an exemplary timing diagram of the data and control signals of the electronic component shown in Figure 2;

Figure 4 is a block diagram of an encryption/decryption cell according to the present invention;

Figure 5 shows the encryption/decryption cell comprising a conditional circuit applicable to the central processing unit according to the present invention;

Figure 6 is a detailed drawing of the encryption and decryption circuits in the cell according to the present invention; and

Figure 7 is a block diagram of a synchronous random signal generator that can be used in the present invention.

Detailed Description of the Preferred Embodiments

Figure 1 shows an exemplary architecture of an electronic security component to which the present invention can be applied. In this example, the electronic component is more particularly designed for smart card type applications. Its external connections are thus limited to two series-connected input/output pads, a clock pad CALK to receive an external clock signal, a pad to receive a resetting signal RST, and the logic supply pads Vcc and Gnd.

The architecture of this component comprises a central processing unit CPU and peripherals P1, P2,

P3 which, in the example, are respectively a non-volatile memory (e.g., an EEPROM type), a RAM type working memory, and a ROM type program memory. An interface circuit INT provides the interface between the serial input/output pads and the parallel bus of the component which is subdivided into an address bus AD-BUS, and a data bus DATA-BUS to which the central processing unit and the peripherals are connected.

In this architecture, it is also planned to have a circuit CAP for access control to the peripheral which receives the most significant bits A7-A5 from the address bus AD-BUS. It contains a space allocation table for the physical addressable space of the component and gives especially the selection signals P1-sel, P2-sel and P3-sel of the peripherals P1, P2, P3 as a function of the decoded address. In this example, the peripherals receive only the least significant bits A5-A0 from the address bus.

Depending on the instructions that the central processing unit receives externally, it gives control signals CTL, especially a read/write signal RW, to be applied to the peripherals. Finally, the pad CALK gives the clock signal PHI applied to all the circuits of the component. That is, the clock signal PHI is applied to the central processing unit, the peripherals, the interface circuit, and the peripheral access control circuit in the example.

In the invention, it is sought to secure this circuit by preventing the determining of the data elements that travel through the internal data bus DATA-BUS through observation of the current consumption of the component. Thus, as shown in Figure 2 in a simplified representation of the architecture of the component of Figure 1, an encryption/decryption cell is placed in the central processing unit and in each of the peripherals that read or write sensitive data on the data bus, i.e., in the peripherals P1 and P2.

These cells are referenced $Kcell_{CPU}$, $Kcell_{P1}$ and $Kcell_{P2}$ in Figure 2.

The electronic component according to the invention then comprises a random signal generator KEY_GEN synchronized with a clock signal on a one-way transmission line to apply this signal to each of the encryption/decryption cells planned in the component. Each of these cells is furthermore connected to the input/output of the data bus DATA-BUS.

Figure 3 shows a timing diagram corresponding to a read operation in which the central processing unit reads a data element of the peripheral P1 followed by a write operation in which the central processing unit writes the data element in the peripheral P1. This timing diagram illustrates the principle of the invention.

This timing diagram shows two clock cycles referenced cycle 1 and cycle 2, the synchronous random signal KIN, the secret key KEY computed locally in each cell, the address bus AD-BUS, the selection signal P1-sel of the peripheral P1, the read/write control signal RW whose low level corresponds to a write command and whose high level corresponds to a read command (by convention), and the data bus DATA-BUS. Considering the first clock cycle shown (cycle 1), it has a corresponding value KEY_0 of the secret key that is computed locally in each cell from the new input value of the random signal KIN, which is 0 in the example.

The peripheral P1 is selected (P1-sel at the high level) in read mode (RW at the high level) at the address applied to the address bus AD-BUS. The cell $Kcell_{P1}$ of peripheral P1 gives on the bus the data element read at this address, which is encrypted with the current value of the secret key KEY_0 that is locally computed by this cell $Kcell_{P1}$. This data element is transmitted on the bus on the low level of the cycle 1 of the clock signal. The encrypted data

element is stored in an input register of the central processing unit CPU on the leading edge of the cycle 1 of the clock signal, and decrypted by the cell $Kcell_{CPU}$ with the current value KEY_0 of the secret key locally computed by this cell $Kcell_{CPU}$.

Considering the second clock cycle shown (cycle 2), it has a corresponding value KEY_1 of the secret key locally computed in each cell from the new input value of the random key KIN, which is 1 in the example. The peripheral P1 is selected (P1-sel at the high level) in write mode (RW at the low level) at the address applied to the address bus AD-BUS. The cell $Kcell_{CPU}$ of the central processing unit gives on the bus the data element to be written at this address, which is encrypted with the current value of secret key KEY_1 that is locally computed by this cell $Kcell_{CPU}$. This data element is transmitted on the bus on the low level of the cycle 2 of the clock signal. The encrypted data element is stored in an input register of the peripheral P1 on the leading edge of the cycle 2 of the clock signal, and decrypted by the cell $Kcell_{P1}$ with the current value KEY_1 of the secret key locally computed by this cell $Kcell_{P1}$.

A general block diagram of an encryption/ decryption cell Kcell according to the invention is shown in Figure 4. This cell is such that it locally computes the current value of the secret key used both for encryption and for decryption. The cell Kcell has a register KEYREG that gives the secret key KEY for the encryption and decryption. It is an n-stage shift register sequenced by the clock signal PHI and receives the random data signal KIN at input synchronous with the clock signal PHI. The register KEYREG gives the current value of the secret key KEY at output for the current clock cycle, whose value is a polynomial function of the n most recent values of the random signal KIN. The

secret key thus takes a new random value at each clock cycle.

The register is preferably a feedback shift register. That is to say, it has combinational logic gates to apply the output bit of certain stages to the input of other stages of the register. This makes it possible to obtain valuable polynomial functions. Preferably, an irreducible polynomial function is implemented to improve the resistance of the encryption.

The cell Kcell has an encryption module A and a decryption module B to which the secret key KEY given by the register KEYREG of the cell is applied. In the example, the mathematical function implemented in the encryption module is the XOR function which has the particular feature of being also the function to be applied in the decryption module and of being easy to implement.

The encryption module A receives inter alia an internal data element Dout from the circuit in which the cell Kcell is placed and the secret key KEY produced locally by the register KEYREG. At output, it delivers an encrypted data element applied to the data bus DATA-BUS through the output interface of the circuit, which is symbolically shown in the figure by a controlled inverter.

The decryption module B receives a data element from the data bus and the secret key KEY locally produced by the register KEYREG. At output, it gives a decrypted data element Din. In one improvement shown in Figure 5, the encryption/decryption cell of the central processing unit comprises, in addition to the elements described here above, a conditional circuit used for the application to the encryption and decryption modules of either the secret key KEY or a neutral key KN corresponding to the neutral value for

the encryption operation considered. In the exemplary XOR operation, this neutral value is the zero value.

This improvement is used to avoid implementing an encryption/decryption cell in all the circuits connected to the data bus in the component considered, and is implemented in only those cells that handle data elements to be protected. It is therefore planned that the control circuit PAC for access to the peripherals (shown in Figures 1 and 2) will give an encryption enabling signal SCRAMBLE to the central processing unit CPU whenever it decodes the address of a peripheral of this kind. In practice, this access control circuit finds this information in its physical address allocation table.

It will be noted that the information SCRAMBLE in the example given by the access control circuit is placed outside or external the central processing unit in the exemplary architecture shown in Figures 1 and 2. This is not absolutely restrictive. The information SCRAMBLE is more generally given by an address decoding circuit of the component.

The conditional circuit of the cell $Kcell_{CPU}$ according to the improvement of the invention comprises a multiplexer MUX receiving the secret key KEY and the neutral key KN at input. At output, this conditional circuit gives the key selected by the encryption enabling signal SCRAMBLE, which is applied to the encryption and decryption modules of this cell $Kcell_{CPU}$.

Figure 6 gives a slightly more detailed view of an encryption/decryption cell according to the present invention. If we consider an 8-bit data bus, the secret key must include at least as many bits. The register KEYREG has eight stages to give eight secret key bits referenced K0 to K7. Each of these eight data bits is applied in the encryption module A, and in the decryption module B to a corresponding XOR gate

receiving the same-order data bit to be encrypted or decrypted at input. Each of these modules thus comprises eight XOR gates, one per bit.

This figure shows an exemplary embodiment of a shift type feedback register KEYREG. The references E0 to E7 designate the eight stages of the register, respectively giving the bits K7 to K0 of the secret key. These stages may be D-type flip-flop circuits, for example.

In the exemplary embodiment shown, the stage E0 receives at input the random signal KIN combined in an XOR gate with the bit K0 given by the last stage E7 of the register, and at output it delivers the bit K7. The stage E1 receives at input the bit K7 combined in an XOR gate with the bit K0. At output it delivers the bit K6. The stages E2, E3 and E4 receive at input the bits given by the preceding stage, and deliver at output the bits K5, K4 and K3 respectively. The stage E5 receives the bit K3 at input which is combined in an XOR gate with the bit K0, and delivers the bit K2 at output. This stage E6 receives the bit K2 at input which is combined in an XOR gate with the bit K0, and delivers the bit K1 at output. The stage E7 receives the bit K1 at input and delivers the bit K0 at output.

Figure 7 represents an exemplary generator KEYGEN of the random signal KIN. In this example, the generator comprises a pseudo-random generator to give a random clock signal that is applied to the D input of a flip-flop circuit BS to be synchronized by the clock signal PHI. This flip-flop circuit therefore receives the clock signal PHI at its clock input, and gives at its Q output a random signal KIN that is synchronized with the clock signal PHI.

It is very difficult in principle to determine the value taken by the random signal by observing the power consumption of the component arising from the switching operations on the

transmission line of the synchronous random signal KIN because the capacitance of this one-way line is very low. However, in one improvement of the invention, it is planned that the generator of the synchronous random signal will comprise a circuit CMC for masking the consumption due to the selection switching operations on this transmission line. In the example, this circuit CMC is connected between the output of the synchronization flip-flop circuit BS and the transmission line.

There are different consumption masking circuits of varying degrees of efficiency. An exemplary non-exhaustive embodiment is shown in Figure 7. It has two D-type flip-flop circuits, B1 and B2. The first flip-flop circuit B1 receives the Q output of the synchronization flip-flop circuit BS as a data input, and the clock signal from the bus PHI as a clock input. The Q output is connected by an interface element (driver) I1 to the transmission line.

The complementary /Q output of the flip-flop circuit B1 is applied to a combinational circuit whose output S is applied to the data input of the second flip-flop circuit B2. The Q output of this second flip-flop circuit B2 is connected to a capacitor CKN whose capacitance corresponds to the parasitic capacitance CK of the transmission line perceived by the output interface I1 of the generator KEYGEN.

The combinational circuit, in the example, has a first OR gate receiving the Q outputs of the synchronization flip-flop circuit and of the second flip-flop circuit B2 as inputs. A second OR gate receives the output of the first gate and the complementary output /Q of the first flip-flop circuit B1 as inputs. With a combinational circuit of this kind, complementary transitions are obtained in the flip-flop circuits B1 and B2 so that the same

consumption due to the transmission of the signal KIN is observed at each clock cycle.

In a another improvement of the invention, it is planned that the random signal KIN will be transmitted on the transmission line only after activation by the central processing unit of an encryption activation signal ENENCRYPT. This can be done simply by forcing the resetting of the flip-flop circuits.

Figure 7 thus shows an AND type logic gate receiving, as inputs, the resetting signal RST of the component which is active at zero, and the enabling signal EN-ENCRYPT. This signal is at zero by default. Thus, so long as the enabling signal is at zero after the setting, the flip-flop circuits B1 and B2 are set at zero, and the transmission line is set at zero. As soon as it is set at 1 by the central processing unit, the random signal is sent.

It will be noted that the two improvements of the generator of the synchronous random signal, namely the masking of consumption and the enabling of encryption, can be implemented independently of each other. Thus, in certain components, it is possible to implement only one of these improvements. To this end, it will be noted that the improvement relating to encryption enabling can be implemented independently of the masking circuit. For example, this may be done using an AND logic gate receiving the synchronous random signal KIN and the activation signal EN-ENCRYPT as inputs, and connected at output to the transmission line.

The use of encryption/decryption cells according to the invention thus gives efficient protection for sensitive data. This protection costs little in terms of design, implementation and processing time for the component. In particular, the design is facilitated by the user of encryption/

decryption cells that are identical in all the peripherals.

The encryption/decryption cell of the central processing unit comprises an encryption-enabling option by which it is possible not to implant a cell necessarily in all the peripherals. The random signal generator has two embodiment options, which are a consumption masking option and an encryption/decryption activation option.